

High-Profile Web Application Attacks

- In the Year 2000 a Norwegian boy attacked a large bank by manipulating the parameters (A/C number) of the URL while making the online transactions.
- On October 31, 2001, the website of Acme Art Inc. was hacked and all the credit card numbers from its online store's database were extracted and displayed on a Usenet newsgroup.
- In June 2003, hackers attacked the Web applications of the fashion label Guess and pet supply retailer PetCo by stealing the credit card information of the customers.

• Citation from <http://www.acunetix.com/websitesecurity/application-scanning-wp.htm>

McAfee

9/21/2007



Protect what you value.

High-Profile Web Application Attacks

- Sept 2007, a Hacker from Sweden had posted email logins and passwords for 100 a/c.s which includes various Embassies across the World & Govt. Offices, on his website.
(www.derangedsecurity.com)

Citation from: Times Of India dated 1/9/07

McAfee

9/21/2007



Protect what you value.

Vulnerabilities in the Database applications

- Data Privacy is important

- What happens when a Database Administration module is vulnerable?

- How do the attackers take advantage of the vulnerable data base admin module?

McAfee

9/21/2007



Protect what you value.

Vulnerabilities in the Database applications

Areas to look into

- Database Connections
 - Unauthenticated updates to a database.
- Table Access Control
 - Table access permissions have to be handled properly.
- Database Access Control
 - Attackers scan for a port that are open by default in the database systems and attack.

McAfee

9/21/2007



Protect what you value.

Vulnerabilities in the Database applications

Scenario: How an attacker journey begins

- Finds server infrastructure and server OS/type
 - Analyses the properties of the server.
 - Scans for the open ports.
- Attacks website/application
 - Attacker looks for feedback/inquiry forms that utilize GET and POST variables.
 - Attacker tries bypassing the logon pages using "authentication bypass" technique.
- Laxity in Input Validation
 - Checks whether the data input is validated or not. If not attacker uses attacks like SQL injection.

McAfee

9/21/2007



Protect what you value.

Attacking Techniques

- SQL Injection
- Cross-site scripting (XSS)
 - Search Engines
 - Error messages
 - User Forms
 - Web Message Board
- Directory traversal attacks
 - <http://www.xxxxxxx.com/abc/def.asp?item=sample.html>
 - <http://www.xxxxxxx.com/abc/def.asp?item=../../WINNT/win.ini>
- Cookie manipulation
- URL manipulation
 - <http://www.xxxbank.com/account?accountnumber=99999&debitamt=1000>
 - <http://www.xxxbank.com/account?accountnumber=34343&creditamt=1000>

McAfee

9/21/2007



Protect what you value.

SQL Injection

- SQL injection exploits web applications that use client-supplied data in the SQL queries.
- SQL injections occur when an attacker is able to insert a series of SQL statements into a query by manipulating data input into an application.

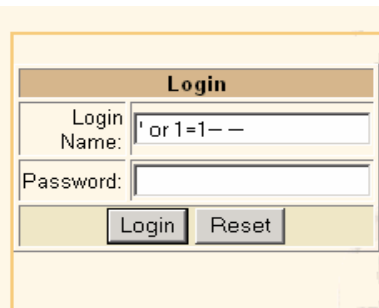
McAfee

9/21/2007

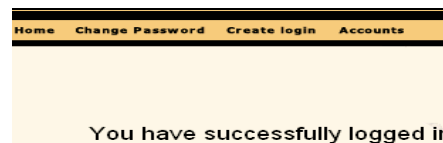


Protect what you value.

SQL Injection



Login	
Login Name:	' or 1=1--
Password:	
<input type="button" value="Login"/> <input type="button" value="Reset"/>	



McAfee

9/21/2007



Protect what you value.

SQL Injection

- **SQL Injection techniques**
 - Redirection and reshaping a query
 - Based on error messages
 - Blind injection

McAfee

9/21/2007



Protect what you value.

SQL Injection

Redirection and reshaping a query

- With this an attacker can enter data into a database, so that the web pages are changed to send a visitor to another website.

McAfee

9/21/2007



Protect what you value.

SQL Injection

Based on error messages

- Attacker sends the malicious data into the client-supplied input fields and expects an invalid SQL query.
- Example <http://www.xxxxxxxxxx/articleid.asp?name=value>
 - Method1: Replace Value by a single quote i.e. name='
 - Method2: Insert a quote in the middle of a value i.e. name=val'ue
- Example error 1:
 - Microsoft OLE DB Provider for SQL Server error '80040e14'
 - Unclosed quotation mark before the character string '51 ORDER BY some_name'. /some_directory/some_file.asp, line 5
- Example error 2:
 - ODBC Error Code = S1000 (General error)
 - [Oracle][ODBC][Ora]ORA-00933: SQL command not properly ended
- Hiding the error messages is not the panacea.

McAfee

9/21/2007



Protect what you value.

SQL Injection

Blind injection

- Trial and error
- Add conditions and know the vulnerability

Attackers gain

- Access to the Database
- Access to servers File system

ONCE DONE NO GREAT DEAL TO REPEAT

McAfee

9/21/2007



Protect what you value.

SQL Injection

<http://www.xxxxxxxx.com/index.php?pageID=5>

From Backend

- SELECT title, description, createDate FROM Content WHERE pageID = 5
- SELECT title, description, createDate FROM Content WHERE pageID = 5 AND 1=1

McAfee

9/21/2007



Protect what you value.

SQL Injection

- Is the current user dbo?
- [http://www.xxxxxxxx.com/index.php](http://www.xxxxxxxx.com/index.php?pageID=5) ?pageID=5 AND USER_NAME() = 'dbo'

McAfee

9/21/2007



Protect what you value.

SQL Injection

- Trackdown the tablename by trying the following queries
- `http://www.xxxxxxxx.com/index.php?pageID=5 AND ASCII(lower (substring ((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'), 1, 1))) > 109`
- `http://www.xxxxxxxxxxxx.com/index.php?pageID=5 AND ASCII(lower (substring ((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'), 1, 1))) > 116`

McAfee

9/21/2007



Protect what you value.

How to safeguard a web application

- Data Validation
- Secure the web application

McAfee

9/21/2007



Protect what you value.

How to safeguard a web application

Data Validation

- Validating the input from unnecessary special characters. Use numbers only where ever it is possible.
- Filter the data with a default-deny regular expression.
- Convert all symbols or punctuation into HTML substitutes, such as "e; or >
- Prevent the use of SQL power characters in user data with out proper encoding.
ex:- 'or ' character String Indicators, -- or # single-line comment, /*...*/ multiple-line comment etc.

McAfee

9/21/2007



Protect what you value.

How to safeguard a web application

Secure the web application

- Limits the rights of the database user
- Use Stored procedures or stored queries to make it impossible for user input to modify the actual SQL statement.
- If possible use any vulnerability assessment tool to automate the discovery of SQL injection and other security vulnerabilities.
ex: Wireshark, Snort, Netcat, Tcpdump etc

McAfee

9/21/2007



Protect what you value.

Thank You

Ganesh_Shastri@mcafee.com

Priya_Darshan@mcafee.com

MadhuMysore_Jayaraju@mcafee.com

McAfee

9/21/2007



Protect what you value.